

(c) Prohibited ESN Alterations -- No person shall remove, obliterate, transfer, alter, tamper with, or otherwise manipulate the original, manufacturer-installed ESN of a cellular mobile station, or otherwise cause a mobile station to transmit an ESN other than the original ESN installed by the manufacturer, except as set forth in subsections (c)(1) through (c)(3) [or (c)(4)]:

(1) Upon the written authorization of a cellular subscriber, the ESN of that subscriber's Primary Cellular Mobile Station may be copied, emulated, or otherwise programmed into one or more mobile stations owned by that subscriber in order to create Secondary Cellular Mobile Station(s), provided that the ESN of the Primary Cellular Mobile Station is not changed, altered or otherwise modified;

(2) The original ESN of a cellular subscriber's Secondary Cellular Mobile Station may be restored upon the written authorization of a cellular subscriber; and

(3) The ESN of a mobile station may be manipulated by its manufacturer or the authorized representative of its manufacturer during the course of repair and upgrade of that mobile station. When a cellular mobile station has been taken out of service and returned to the manufacturer, the manufacturer may reprogram that cellular mobile station with a new ESN in order to resell it after it has been restored to proper working order.

[(4) Where the subscriber's ESN has been incorporated into a hardened, separable, subscriber identity module ("SIM") which also embodies the industry standard authentication data and processing as set forth in subsection (b)(1), the subscriber may physically move the ESN by moving the SIM from one mobile station to another provided that:

(i) both mobile units are designed and equipped to operate with a SIM;

(ii) the ESN in the SIM is not changed, altered or otherwise modified; and

(iii) the SIM properly identifies the subscriber for billing purposes.]

(d) Extension Service Provider Requirements -- Any person performing any ESN procedure permitted pursuant to subsections (c)(1) and/or (c)(2), must comply with the following requirements:

(1) Prior to performing any ESN procedure authorized pursuant to subsections (c)(1) and/or (c)(2), the Extension Service Provider must: (i) notify the operator of the subscriber's home cellular system by telephone and/or facsimile that the subscriber has authorized such ESN procedure; and (ii) provide the subscriber with a copy of subsection (e) of this section.

(2) The notice to the system operator required by subsection (d)(1)(i) shall provide the system operator with the subscriber's name, address and mobile identification number(s); the make, model and ESN of the affected cellular mobile station(s); the name and address of the Extension Service Provider performing the procedure; and the rule provision pursuant to which the procedure is being performed.

(3) The Extension Service Provider shall refuse to perform any ESN procedure for a customer and shall retain a copy of any identification provided by the customer if the carrier, at the time of the notice required pursuant to subsection (d)(1)(i), immediately informs the Extension Service Provider that the customer:

(i) is not a currently authorized subscriber to the carrier's cellular system;

(ii) is not authorized to use the Primary Cellular Mobile Station identified by the customer on the carrier's cellular system; or

(iii) has identified as his or her Primary or Secondary Cellular Mobile Station a cellular mobile station which has been reported to be stolen.

(e) Operation of Cellular Mobile Stations -- Simultaneous operation of Primary and/or Secondary Cellular Mobile Stations emitting the same MIN/ESN combination is prohibited and is cause for suspension of service by the carrier. Where service has been suspended by the carrier pursuant to this provision, a subscriber may be required to pay a re-activation charge which shall not exceed the lowest service initiation charge assessed by the carrier for a single mobile station.

(f) Obligation to Provide Service -- A cellular carrier may not deny service to a cellular subscriber based on the subscriber's use of one or more Secondary Cellular Mobile Stations, except where service is suspended pursuant to subsection (e), and may

not refuse to restore service if the subscriber pays the re-activation charge pursuant to subsection (e).

(g) Unauthorized Interception of ESN Transmissions: -- No person other than the licensed operator of a cellular base station shall: (i) transmit signals to a mobile station, regardless of the level of transmitted power used, which cause the mobile station to transmit its MIN, ESN, random challenge-response data, or other billing identification variable; or (ii) intercept the transmission of the MIN, ESN, random challenge-response data, or other billing identification variable of a cellular mobile station, except where such interception is authorized by an order issued by a Court of competent jurisdiction. This subsection (g) shall not apply to: (i) procedures used by a manufacturer, or the authorized agent of a manufacturer, engaged in the repair of a subscriber's mobile station pursuant to written authorization from the subscriber; or (ii) a subscriber's use of a low power home base station properly authorized by the Commission which enables the subscriber to use a cellular mobile station as a cordless telephone.

ICSA

Attachment 3

Independent Cellular Services Association

P.O. Box 2171 • Gaithersboro, MD 20886 • Phone 301- [REDACTED] • FAX 301- [REDACTED]

August 11, 1995

Mr. William F. Caton, Secretary
Federal Communications Commission
1919 M Street, N. W.
Washington, D. C. 20554

Re: Petitions for Reconsideration in CC Docket No. 92-115
Ex Parte Discussion

Dear Mr. Caton:

This is to provide notice, pursuant to Section 1.1206 of the Commissions's Rules, that we have mailed the attached letter to Ms. Keeney regarding our motion for reconsideration for Part 22.919 of the FCC rules.

This letter to Ms. Kenney and its attachments were requested at a July 27, 1995 meeting that we attended with members of the Commission, CTIA, TIA, and C2+.

Sincerely,



Michael G. Heavener
President MTC Communications
Vice-President ICSA
For CellTek

Attachments

ICSA

Independent Cellular Services Association

P.O. Box 2171 • Gaithersboro, MD 20886 • Phone 301-926-1891 • FAX 301-670-0234

August 11, 1995

Regina M. Keeney, Esquire
Chief of the Wireless Bureau
Federal Communications Commission
2025 M Street, N.W., Room 5002
Washington, DC 20554

Dear Ms. Keeney,

Subject: Ex-Parte Meeting regarding Part 22.919 - ESN
rule and Extension Cellular Phones

We were disappointed that you were unable to stay for the meeting on July 27, 1995 regarding our Ex-Parte Presentations which addressed our petitions for reconsideration of the ESN rule in Part 22.919. We are forwarding a copy of this letter to Mr. Caton, Secretary of the Commission to officially put this letter and its attachments on the record. For that record, attendees included representatives from the FCC, McCaw/AT&T Cellular, TIA, C2+, MTC Communications, CellTek, ICSA, Motorola, Ericsson, Japan Radio, Matsushita Electric and the Department of Justice Antitrust Division. This letter summarizes the major points that we concluded from the meeting and we have attached a rewrite of Part 22.919 as your staff requested:

1. According to Paragraph II A. of the agenda and opening comments of Mr. B. C. "Jay" Jackson, Jr. of the Commission, Part 22.919 and related comments apply to the carriers who are cellular licensees and to "the design criteria to be met by manufacturers as a condition of type acceptance ...". The rules do not apply to firms such as ourselves who do cellular phone reprogramming. CTIA and the comments in the current part 22.919 suggest that we cannot change ESN's because we somehow void type acceptance. In our petitions and during our presentation, we quoted the Commission's own rules for type acceptance which permit minor technical changes to radio transmitters without voiding type acceptance. The ESN is merely transmitted information and in no way affects the power, frequency, modulation, etc. of the transmitter which are contained in the technical standards

cited in the type acceptance rules. We are using for the the same programming access ports that cellular companies and service facilities have been using for many years to change ESN's in the field. The largest cellular manufacturer, Motorola, call this feature "Express Service" or "ID Transfer". We are still willing to work with you on the language of the rule even though we don't think it applies to us or our associates.


2. Mr. Michael Altschul stated that CTIA could not find any major disagreement with the technical report filed earlier by Dr. Richard Levine who testified for the extension phone companies. Dr. Levine's report concluded at least three major points: a. that phones programmed with duplicate ESN and MINS do not "burden or harm the network or other subscribers" if the phones are used properly; b. "There is no problem of incompatibility or interference with anti-fraud techniques"; c. "the use of emulated extensions provides a technologically superior method for providing extension service". We believe that all in attendance agreed that there is no technical basis for the commission not permitting an ESN change in the field if a customer requests an extension phone or a needs a loaner phone.

3. TIA representing the manufacturers stated that they dislike the current rule 22.919 and believe it is written so strictly that it is impossible to comply with for normal repair and software updates of cellular telephones in the field. Both TIA and our members don't believe the rule will have any significant impact on fraud because there are 30 million existing phones which are not covered by the new rule. Mr. Raclin(for TIA) stated that if the rule is left in place then the manufacturers will be unable to provide field software updates and repairs which will result in phones being thrown away resulting in major customer inconvenience and expense. Incredibly CTIA stated that they are aware of this issue and are willing to create these problems for their subscribers -- as we testified, CTIA and their members stand to make billions of dollars of revenue from rolling out their own extension phone service. We believe that they want to monopolize this market and this is the real reason they are opposed to customer authorized ESN changes. With the extensive theft-of-airtime problems so often brought up by CTIA and its members, the ESN has proven to be totally ineffective as a security measure.

4. CTIA submitted two extensive volumes of material at the beginning of the meeting which basically demonstrated their assault on a number of small firms performing ESN modifications. CTIA and several carriers using the FCC rules under reconsideration have obtained Federal Court injunctions to put these firms out of business. In our meeting, CTIA attacked C2+ on several occasions using deceitful tactics such as referring to criminals who were caught stealing cellular services as "using C2+ type technology". In fact the technology is adapted from that used by the manufacturers to read and write the ESN at the end of the manufacturing process or to change the ESNs in the field. In all of the thousands of pages submitted in this reconsideration and the 6 cases in the large binder passed out at the meeting, there was not a single example where C2+ or any other extension firm altered a cellular phone used in the stealing of airtime. Despite this fact CTIA and McCaw continued to try to confuse the Commission by mixing true fraud with extension service provided to legitimate customers who request the service. It was pointed out by us that CTIA had succeeded in having the Congress revise Title 18 of the U.S. Criminal Code to make it a felony to alter phones to "free ride" on the cellular system. We believe this is more than adequate Federal regulation to deter true fraud.

5. There was extensive discussion relative to the extension phone service(MUSDN) that the carriers are offerings in a number of markets. We pointed out that the carrier's service is priced between \$18 and \$30 per month as contrasted by our service which averages about \$3 per month(one time cost amortized over 5 years). The carrier's extension service is termed MUSDN. It was pointed out that the carriers require that only one phone be powered on at a time; this is the same requirement that our members require of our customers. We also pointed out that under MUSDN as provided by the carriers only the primary phone can roam which is a clear violation of the commission's compatibility standards. All of our phones can roam. Furthermore MUSDN is available in only a few markets. Our service can be provided in ALL MARKETS large or small!

6. C2+ and MTC Communications pointed out that the Commission, CTIA and TIA failed since the mid '80's to enforce the rules that required all cellular telephones be designed to prevent the ESN from being changed. The rules dating back to the early 80's specified that should an ESN be changed then the phone would be rendered useless. This is

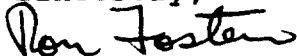


clearly not the case! As stated earlier the carriers and manufacturers have developed a process where they can easily change any ESN in the field. This technology is now available to anyone who wants to purchase it. With 30 million phones in the marketplace most of which can be reprogrammed in seconds, the FCC ESN rules would have virtually no impact on fraud. TIA agreed with us. Instead the industry needs to turn to PIN numbers, usage patterns and authentication to curb fraud and away from a failed dependency on controlling the ESN.

7. Finally, at the conclusion of the meeting, the Commission members requested that C2+ and our association/firms draft a set of rules that would be fair to all parties and submit to the Commission within two weeks. The Commission would then consider our suggestions for the reconsideration of the existing rules in Part 22.919. We have attached our ideas to this letter together with some comments which explain our logic for the rules we are suggesting. We believe that our proposed rules place a number of safeguards on the cellular extension service industry so that the firms providing this service will CONTINUE to provide an affordable service without contributing at all to fraud. In short, we can live with the existing rule provided paragraph a.) be clarified to mean that "in service" is powered on. Also paragraphs 60 to 62 in the comments, the FCC Public Notice, Report No. CL-92-3 issued in 1991 and the letter from John Cimko in 1993 to CTIA need to be struck or clarified to address only the ESN changes that are done fraudulently without the customer's permission.

We know the marketplace demands cellular extension service and therefore we believe that our service is technically and economically in the best interest of the public. It also adds a form of competition to the marketplace and we are convinced that this is why CTIA and the carriers have been so resistant to our service. We would like to thank you and the other members of the Commission for arranging this meeting and we are hopeful for a positive outcome for our petitions.

Sincerely,



Ron Foster

Combined response for CellTek, MTC Communications, and ICOSA

Attachments

Attachment 3-A

Attachment A

PROPOSED RULE SECTION 22.919

a.) Definitions

1.) ESN -- The Electronic Serial Number(ESN) is a 32 binary number that uniquely identifies a cellular customer's primary mobile transmitter to the cellular system to verify that he/she is a valid customer.

2.) Primary Phone -- Each primary cellular phone in use must have a unique ESN that was preassigned or installed at the factory. This ESN together with the MIN are the numbers that were registered with the carrier at the time of service activation. This ESN must not be changed except by the manufacturer or with written permission of the relevant carrier.

3.) Secondary Phone -- Each secondary phone must be programmed with the same information as the primary phone in 2.) above at the written request of the customer owning the primary phone. This phone can be used as an extension phone or as a loaner phone while the primary is being repaired. The secondary phones must be owned by the same person as the primary phone.

4.) Programming Service Provider -- This is the firm that reprograms a new ESN in each of the Secondary Phones.

b.) Operation of the Phones

Only one cellular phone, either the primary or a secondary, may be powered on at a time. This must be explained both verbally and in the written agreement between the owner of the primary phone and the programming service provider. Should the carrier detect that two or more phones with the same information are on at the same time, then the carrier may suspend service and require a fee for reactivation after notification.

c.) General

1.) A service agreement between the owner of the phones and the service provider must be signed by the owner of the primary phone. This record must contain all relevant information on the owner of the phones including name, address, telephone numbers, Primary ESN, old ESN for each secondary phone, information on two sources identification, makes and models

of phones, carrier and a copy of a valid service contract with the active carrier. These records must be maintained as long as the secondary phones are in operation. Upon request the relevant carrier may gain access to the information in this agreement.

2.) Each time a secondary phone is programmed, the primary phone customer must produce that phone in person, show a valid contract with a carrier, and provide proper identification. The firm providing the programming service must notify the carrier who provides the primary phone service that a secondary phone is being created. If there is a problem with the customer or the account then the programming service should be denied. The carrier must not take any punitive action against the customer or the firm providing the service nor create any delay in responding to the programming service provider notification.

3.) A tag with the new ESN must be placed along side the existing ESN plus the name, address and phone number of the firm providing the reprogramming service.

4.) Any company providing programming service of a secondary phone must have a valid business license and perform services within the geographic area served by the home carrier. Mail order service outside this area should not be allowed under this rule. As stated earlier, physical identification of the subscriber and the primary phone is required.

5.) Programming service companies performing this service should notify local carriers of their operation so that coordination of problems can be made.

6.) To assure proper operating conditions of the secondary phones the firms providing this service must have one employee on it's staff that has at a minimum a 3rd Class Radio Technician license. This license can be revoked should any fraud or other major problems with the reprogramming service be proven. The service firm must strictly follow the process outlined in this rule or a failure to do would be grounds for suspension.

7.) All equipment and software used for the purposes of reprogramming ESNs must have restricted access such as passwords or other security locks to prevent unauthorized or fraudulent use. The equipment/software used by the firms programming secondary phones must be under the direct control of the firm providing the service.

8.) All cellular telephones submitted for type acceptance within 6 months after this rule is published shall be designed to include the authentication standard xxxx.

9.) No individual or company shall modify, transfer, copy or alter an ESN emitted by a mobile cellular transmitter except as set forth in the above paragraphs a.) to c.). Any individual or company not in compliance with these subsections is in violation of the rule and the Act.

Certificate of Service

I hereby certify that a copy of the foregoing letter to Regina M. Keeney and all exhibits were mailed this 14 day of August , 1995 by first-class mail, postage prepaid, to the following parties:

Rosalind K. Allen
Acting Chief
Commercial Wireless Division
Wireless Telecommunications Bureau
Federal Communications Commission
2025 M. Street, N. W., Room 7002
Washington, D. C. 20554

Steve Markendorff
Chief, Broadband Branch
Commercial Wireless Division
Wireless Telecommunications Bureau
Federal Communications Commission
1919 M. Street, N. W., Room 650
Washington, D. C. 20554

Sally Novak
Chief, Legal Branch
Commercial Wireless Division
Wireless Telecommunications Bureau
Federal Communications Commission
2025 M. Street, N. W., Room 7002
Washington, D. C. 20554

B. C. Jackson, Jr.
Engineering Advisor to the Chief
Commercial Wireless Division
Federal Communications Commission
2025 M. Street, N. W., Room 7002
Washington, D. C. 20554

Barbara Espin
Commercial Wireless Division
Federal Communications Commission
2025 M. Street, N. W., Room 7002
Washington, D. C. 20554

Daniel B. Phythyon
Sr. Legal Assistant to Chief
Federal Communications Commission
2025 M. Street, N. W., Room 7002
Washington, D. C. 20554

Mr. Tim Fitzgibbon
Attorney for C2+
Carter, Ledyard & Milburn
1350 I Street, N.W.
Suite 870
Washington, D. C. 20005

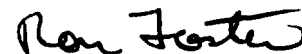
Mr. Michael F. Altschul
Chief Counsel
CTIA
1250 Connecticut Av. N.W.
Suite 200
Washington, D. C. 20036

Brent E. Marshall
Antitrust Division
U.S. Dept. of Justice
555 Fourth Street, N.W.
Washington, D. C. 20001

Cathleen A. Massey
McCaw Cellular
1150 Connecticut Av. N.W.
4th Floor
Washington, D. C. 20036

Grier C. Raclin
Attorney
Gardner, Carton, Douglas
1301 K. Street, N.W.
Suite 900, East Tower
Washington, D. C. 20005

John W. Berresford
Office of General Counsel
Division of Competition
FCC, Room 500D
2033 M. Street, N. W.
Washington, D. C. 20554



Ron Foster

Set Yourself Free With FlexPhone: The Flexible Choice in Cellular Service

FlexPhone is a new service from Cellular One that lets you direct calls on your cellular number to any one of up to 3 cellular phones. FlexPhone is not an extension phone nor will it allow two people to use the same number. Designed to make staying in touch easier, FlexPhone is ideal for someone already enjoying the hands-free convenience of an installed car phone, but wants a portable to use outside the car. The following information will help you decide if FlexPhone is right for you:

How Does FlexPhone Work?

Once you have decided whether one or two additional phones will compliment your lifestyle, call Cellular One or an Authorized Dealer to initiate your FlexPhone service. After activation, you decide which phone to receive calls on and simply turn the others "OFF". When a caller dials your number, the phone that is "ON" will ring. The FlexPhone feature will not function properly if both phones are "ON". Now, your calls can follow you from your car, to meetings, on errands or nearly anywhere else.

What About Roaming?

When you activate your FlexPhone service, you'll designate the phone you plan to use outside the Baltimore-Washington coverage area as "Primary" and the other(s) as "Secondary". That's it—your cellular service is ready to travel with you on your "Primary" phone. You cannot use your "Secondary" phones to roam unless you first redesignate your FlexPhone service with Customer Care. (There's no charge for redesignation. May take up to 48 hours to complete.)

Can Two Phones Sharing One Number Call Each Other?

No, since only one phone will operate at a time, you can't use FlexPhone to call between phones sharing the same number. To accommodate this, you would need to use the full value of two Cellular One phone numbers.

Two Ways to Start Enjoying FlexPhone

FlexPhone service is available for Cellular One customers that want to operate two or three cellular phones with the same cellular number. The following FlexPhone pricing is effective for customers using any Cellular One rate plan in addition to their current rate plan monthly fee:

• Two Phone Service

Add one extra phone to your Cellular One service for \$17.95 per month.

• Three Phone Service

Add two extra phones to your Cellular One service for \$29.95 per month.

(Additional fees for activation of second and/or third phones are not required. Up to 48 hours may be required for FlexPhone activation. Regular air-time charges and applicable sales taxes apply. All calls are billed to one number on the same bill. Detailed billing will not distinguish which phone made a call.)

Ask Your Cellular One Representative for Details

To learn more about FlexPhone or about our commitment to providing the best products, service and value available, ask your local Cellular One dealer or call *611 (free from your cellular phone) or 1-800-CELL-ONE.

Attachment 5

One Number.

Our New 2 Phones/1 Number™ Service Lets People Call Either Of Your Cellular Phones With Just One Number.

It's commonly known that cellular phones do have much in common. But never before have they shared this singularly exclusive item.

2 Phones/1 Number™ service.

Which means people can reach you at either your mobile or portable cellular phone by dialing just one cellular number.

No other cellular company makes it so easy to be so accessible. And also, to be so productive.

The bottom line is, calling you is much easier. For your clients, business associates, friends and family. Because they have just one number to call.

Suddenly, you're more available. You're easier to find. You're staying in touch and on top.

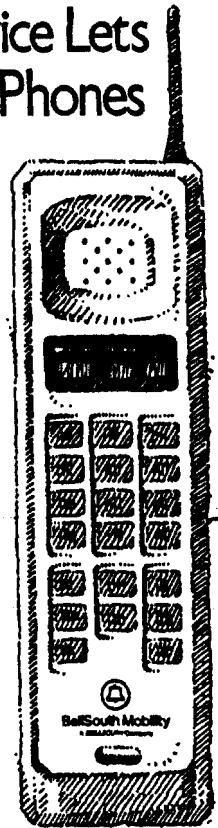
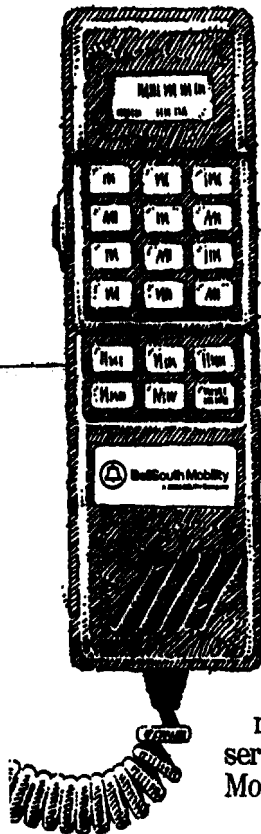
And to make matters even easier, you receive just one bill for your two phones.

So talk about our new 2 Phones/1 Number™ service with your BellSouth Mobility representative today.



BellSouth Mobility
A Bellsouth Company

Phones featured by Motorola.



To be completed by your BellSouth Mobility representative at time of activation.

Customer acknowledges that he/she has read and understands the terms and conditions of this program set forth on the reverse side of this brochure and agrees to be bound by them.

BELLSOUTH MOBILITY INC

AUTHORIZED USER

NAME _____

NAME _____

TITLE _____

TITLE _____

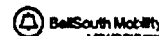
The Works On How 2 Phones/1 Number Service Works.

Terms And Conditions

- 1) To take advantage of this new service, simply sign a 12-month Service Agreement for any existing or additional line (\$200 cancellation fee).
- 2) 2 Phones/1 Number service costs \$39.00 per month in addition to monthly access and airtime charges.
- 3a) If you're a *current BellSouth Mobility customer with two existing cellular numbers*, the cost to activate the 2 Phones/1 Number service will be \$30.00 (one-time charge).
- 3b) If you're a *current BellSouth Mobility customer with one existing cellular number or a new BellSouth Mobility customer*, you'll be charged a \$40.00 activation fee (one-time charge).
- 4) 2 Phones/1 Number service is designed to be used by one person. If two people share one cellular number, situations could arise in which incoming calls could reach the wrong party or even be unanswerable.
- 5) Only one phone can be turned on at any one time. If both phones are left on, you may not be able to answer your incoming calls.
- 6) One phone must be designated as the primary phone, and only that phone can be used for roaming. Switching your primary phone designation is easily done by calling Customer Service and paying a \$30.00 charge.
- 7) If you have a horn alert on your vehicle, you'll need to disengage the alert when you have your portable phone on.

BMI does not assume and shall have no liability under this Agreement for failure to provide or delay in providing service for the Equipment due directly or indirectly to causes beyond the control of BMI, including, but not restricted to, acts of God, acts of the FCC, acts of public enemies, acts of the United States, any State, Territory of the United States, or any political subdivision of the foregoing, or the District of Columbia, acts or failures to act by the Customer, its agents, employees, or subcontractors, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes, and unusually severe weather conditions, or defaults of BMI subcontractors due to any such causes.

Customer shall indemnify, protect and hold harmless BMI and its officers, employees and agents from and against any and all claims, actions, proceedings, losses, damages or liabilities (including without limitation attorneys' fees) arising in any way in connection with this agreement and the Equipment, including without limitation, manufacture of Equipment, its selection, purchase, delivery, possession, use, operation or return and the recovery of claims under insurance policies thereon. This indemnification shall survive the termination of this Agreement.



To be completed by your BellSouth Mobility representative. Please keep this brochure for your records.

ESN: PRIMARY PHONE (USED WHEN ROAMING) _____
 DESCRIPTION _____
 ESN: SECONDARY PHONE (NOT USED WHEN ROAMING) _____
 DESCRIPTION _____
 CELLULAR NUMBER (_____) _____
 RATE PLAN _____

Introducing A Feature Never Before Shared By Two Cellular Phones.



Richard C. Levine, Sc.D., P.E.
Beta Scientific Laboratory, Inc
P.O. Box 836224
Richardson, TX 75083-6224
telephone 214 233 4552
(area code changes from
214 to 972, September 14, 1996)

July 30, 1996

Ms. Michele Farquhar
Chief
Wireless Telecommunications Bureau
Federal Communications Commission
2025 M St. NW, Room 5002
Washington, DC 20554

Re: CC Docket No. 92-115
Informal Submission: Rebuttal of Technological
Errors in May 1996 CTIA and AT&T Wireless Submissions
Regarding Rule 22.919

Dear Ms. Farquhar:

Background: I am a telecommunications consultant, and university professor of Electrical Engineering and telecommunications. I was retained in 1995 by C2+, a former petitioner in this docket, to prepare a report on emulated cellular extensions, which was submitted to the Commission on July 7, 1995, and I also attended a meeting at the Commission on July 27, 1995, at which the other petitioners, CTIA and AT&T Wireless Services (AWS), and other participants as well, stated that they had no disagreement with the technological statements presented in my 1995 report. This agreement by CTIA and AWS is significant because my 1995 report directly contradicted and rebutted numerous technological assertions made by both of them in previous filings as the basis of their position. My qualifications as an expert on the technology and operations aspects of cellular and wireless systems were stated in an attachment to the 1995 report.

In May 1996 I saw two additional documents: one filed by the CTIA (dated May 16, 1996) and the other by AT&T Wireless Services (dated May 3, 1996). These documents oppose any changes in Rule 22.919 which would permit alteration or copying of the ESN in a cellular telephone for both extension use (which these two parties have consistently opposed) but also for any other purpose whatsoever, such as replacement of a faulty cellular phone by a repair depot. Soon after, I learned that C2+ was out of business and had agreed, as a condition of settling a lawsuit with the CTIA, that they would drop their petition to the Commission in this docket. After long and careful consideration, I am submitting this informal letter representing only myself and my own views. I have no employer or sponsor whom I represent in this matter.

I am submitting it for several reasons: First, one important effect of a complete prohibition on ESN copying or transfer is to prohibit implementation of the most effective and proven unbreachable form of the industry standard authentication algorithm. This is my main concern, since I have devoted several years of my professional career and my own personal time and expense to developing a truly secure method to prevent fraud, and I am distressed to see its effectiveness diluted due to apparently widespread technological misconceptions and consequent ill-advised actions about the technology of anti-fraud measures. I have no personal or business financial interest whatsoever in the promoting the use of the authentication algorithm, and I have no property rights in the relevant patents or associated technology and am in fact, likely to make more as a technological consultant if I am called on to fix problems created by the continued absence of this technology. I am sadly compelled by the facts to conclude that the present position of the CTIA and AWS, calling for a complete prohibition of ESN transfer, greatly weakens the arsenal of technological capabilities against fraud, and is clearly irreconcilable with their stated motive of fraud prevention. Second, several new false technological assertions are made now by both CTIA and AWS, which require correction so the Commission can reach a decision based on fact. Third, a number of previous false assertions, already rebutted fully in my 1995 report which was agreed to by CTIA and AWS, are again resurrected by them both using different wording. In particular, the most egregious of these false statements arise from a complete misstatement of what I said in my 1995 report about authentication and/or the false claim that emulated extensions have degrading effects or require complex further network development, when the truth is precisely the opposite in several senses of the word. These misstatements of what I said are so severe that, if not promptly and widely countered with the facts about what I said and implied, they could be damaging to my professional reputation when seen by competent

people in the industry. Finally, I fear that if I do not speak out, there is then nobody left to speak for the consumer of cellular services who wants multiple cellular phones with the same MIN (directory number). Under the present Rule 22.919, this consumer will be left with only the inferior and more costly MUSDN service offered by several cellular carriers. In fact, from my own point of view, the dispute between the opposing past and present petitioners on both sides appears to be molded more clearly by economic considerations and competition for the "extension" market, than by considerations of preventing fraud.

I am greatly distressed by the CTIA and AWS documents, primarily because the preponderance of the assertions made by both consist of extremely serious technological errors and incorrect statements. These statements are particularly distressing because both CTIA and AWS each have readily available some of the best-informed technological experts in the cellular industry, any of whom could have been called on to make a correct expert statement about the relevant technology. Not all of their technological statements are false, of course, but those which lead to their conclusions are almost all false. Furthermore, it has come to my attention in June that, while these cellular operator petitioners are opposing all exemptions to a prohibition on alteration of the ESN, a large number of cellular operators have been using or encouraging the use of a different type of cellular telephones (the Cellemetry ® system, discussed below) which clearly intentionally violates both the present form of Rule 22.919 and also the previous Rule 22.933. No exemption has been requested by them for this equipment, even though it truly has the potential to produce degradation of the cellular network in some of the very same ways which were falsely alleged by the CTIA and AWS in their prior filings opposing emulated extensions.

I have numbered the technological assertions which I have identified in the two cited documents, and present my comments and rebuttal to each, and then finally my conclusions and recommendations regarding Rule 22.919. I apologize that so much of this material again considers matters already considered in detail in my 1995 report, but this is necessary in several cases to show that many assertions which I respond to here are merely restatements of previously rebutted assertions, which were restated in the cited two letters to appear like a new or non-rebutted facts, when in fact they are not.

1. The CTIA asserts (pages 2-3) that, after 16 months of experience under the wording of Rule 22.919 which became effective January 1, 1995, experience and hindsight have shown that: a) there is no need for the FCC to mandate a requirement for authentication in newly type accepted handsets, because the CTIA is confident that no rule is needed to make authentication available in all (or nearly all) markets, and b) the alleged "adverse affect" [sic., should be "effect"] on manufacturer's repair and upgrade of cellular telephones in the field have not materialized.

1a. Regarding point a): The long delay (from 1991 to 1995) until a policy statement was issued by the CTIA demanding authenticating cellular phones is partially due to a so-called "self-fulfilling prophecy." The 800 MHz cellular carriers were first dubious about the efficacy of authentication, partly because 10 million non-authenticating sets were then already in use, and zero authenticating sets. There were also some persistent technological misunderstandings regarding the specifics of authentication, some of which are repeated by AWS in the recent letter. Since carriers were dubious about its efficacy, they did not unite in demanding that all new sets be authentication-capable. Then, because the number of sets without authentication was growing, the lack of support for authentication continued. Finally, in 1995 the vicious circle was broken for the first time and the CTIA deserves full credit that a policy was then introduced to demand authentication capability in new 800 MHz cellular phone introductions. However, this is not an irreversible policy. It is still not a position enthusiastically supported by all member carriers of the CTIA, and many of its member carriers have not consistently supported the use of authentication in the past and have no obligation to do so in the future. This is why the CTIA can only promise that "nearly all" [emphasis added] cellular markets will have it.

Authentication is 100% Technologically Effective, Yet the Cellular Operators are not 100% Convinced: Authentication has been proven by European experience to be 100% effective against technological fraud, but only when it is 100% deployed in all cellular phones and base systems. In contrast, American carriers have tried repeatedly to use anti-fraud methods which are acknowledged to be both highly "porous," (they only identify a fraction of the actual fraud, not all of it) and also have high "false denial of service" rates (they deny service to some valid customers). In contrast, authentication has been proven by European experience to be free of these two faults. During the 5 years since TIA authentication was standardized the population of American cellular phones has grown from about 10 million to about 25 million, and the cellular operators have been delaying a firm decision on the use of authentication, while restlessly flitting from one only partially effective method to another, searching for the elusive "silver bullet" which will consistently deny service to fraudulent cellular phones yet never deny service to legitimate phones. No clear schedule priority was presented to manufacturers of switches and network equipment to roll out authentication in the network, and no concerted industry wide effort has been organized to test and verify network wide compatibility. (The industry can do this when it wants to, as shown by the highly successful "Lockdown" coordinated testing and verification process performed to introduce the IS-54 Digital cellular standards.) Given this history, I suggest that it is essential to protect the interests of everyone (carriers, consumers, etc.) that 100% implementation of authentication in new cellular phones be mandated on a

reasonable and achievable calendar basis by the Commission, rather than leaving this to the choice of the cellular operators alone. In my highly biased opinion, this historical delay and indecision has been a major factor in bringing us to the present situation, which has given criminals a long-term free hand to steal service and use cellular phones to further their other criminal enterprises.

Lack of Mandated Authentication Discriminates Against Authentication vis-à-vis Other Anti-Fraud Methods: There is no reason for the Commission to deny any particular possibly valuable anti-fraud technology its opportunity to be applied. Carriers should have the option of using any and all anti-fraud technologies available, particularly when each has its own particular interval of effectiveness or sphere of application. Consider the objections which would be raised if the Commission passed a rule which was prejudicial toward just one other anti-fraud technology. For purposes of discussion, I will mention two apparently useful rule changes which also have adverse effects on fraud control. Imagine the quite valid uproar of objections if the Commission mandated a tight time-domain mask on the cellular control channel frequency shift keying (FSK) signaling waveform to reduce out of channel RF emission, and thereby increase cellular system capacity slightly. Although that ostensible objective could indeed be achieved, this would also have the secondary effect of crippling RF fingerprint or signature anti-fraud technology, since incidental unit-to-unit differences between different sets would also become more subtle and difficult to detect. Similarly, imagine the valid objections if the Commission introduced a rule to limit or restrict the number of digits which could be dialed by a cellular phone following initial connection. This might prevent certain types of conference call dialing errors, but it could also cripple PIN entry as an anti-fraud method. Other examples are conceivable, but all are equally silly, and of course I present these examples only to illustrate that a well-intentioned technological proposal in a complex system like the cellular network can often have unexpected collateral negative effects on combating fraud. In each of these cases, the ostensible benefit of the proposed change must indeed be a very significant contribution to the public interest, convenience and necessity in order to justify the reduction in fraud protection which it produces. I suggest to the Commission that the proposal by CTIA and AWS to not mandate authentication in new set production and to unconditionally prohibit ESN copying or transfer fail this test. Lack of mandated authentication in cellular phones makes ultimate effective use of authentication dependent on the historically demonstrable strongly divided and fickle sentiments of the carriers, and prohibition against ESN transfer prohibits the most secure implementation of authentication (discussed further below). It significantly reduces the best security level of the industry while raising the cost and reducing the quality of service to extension customers, and gives no anti-fraud benefits to compensate for these detriments.

Prohibiting ESN Transfer Prevents the Most Secure Implementation of Authentication: The new position of the CTIA and AWS (now opposing any changes in the ESN) "throws the baby out with the bath water" by consequently forbidding the most technologically secure form of authentication, namely implementation in a separable authentication chip (packaged as a so-called "smart card" or "smart SIM chip"). While the CTIA and AWS are fully entitled to take any position in this debate, including reversal of their position on any point at any time, this particular new position appears to me to be technologically the worst possible position of all for 800 MHz cellular service, since it leaves only the weaker form of implementation of authentication (via combined or "one-piece" software with call processing) available for US use, and is thus clearly inferior to PSC-1900 and other competitive systems with a separable authentication chip. Rapid implementation of the separable chip form of authentication will not only give an unbreachable physical security to the A-key and other secret information, but it will also automatically solve the repair/replacement issue described in the next section, for cellular phones equipped with a separable chip.

1b. Regarding point b): While there is no substantiating supporting data presented by the CTIA for their assertion that none of the concerns regarding set repair and replacement have materialized. I ask for substantiating background information because my own knowledge of the industry indicates that cellular telephone set replacements are still being done extensively via changing the ESN of a replacement set, while everyone concerned merely ignores these violations of Rule 22.919. My impression of the situation may be correct or incorrect, and even if it is correct it does not necessarily imply an explicit conspiracy of silence on the part of anyone. However, if there indeed has been no problem since January 1, 1995, and "business as usual" together with "don't ask, don't tell" is not the true explanation, then one of the following things may have occurred:

- 1b.1 The reliability of cellular phones has suddenly magically increased so that no repairs are required.
- 1b.2 A new method of instantaneous repair, not previously reported to the public or to the technologists, has been put in place.
- 1b.3 Cell phones are being repaired at the normal speed, but customers don't mind being without them for hours to days, and have made no complaints.
- 1b.4 Cell phones under repair are temporarily replaced by "loaner" phones having a different telephone number (MIN) and ESN, but the customers do not have any objections to the inconvenience of advising all their associates of their new telephone number, and have made no complaints.

1b.5 Cell phones under repair are being replaced by replacement sets coded with the original directory number (MIN) but, of course, having a different ESN than the non-working original set, and are being instantly activated by the carrier without charge to the consumer. This, if it is the reason, is a particularly generous act by the carriers, in view of their prior assertion that the emulated extension customer is merely trying to illegally evade an activation charge for a second cellular phone.

Of course, I propose items 1-2 only in jest and sarcasm, but items 3-4 are only half in jest, and item 5 is quite possible, although it indicates a serious inconsistency in the prior arguments of the CTIA. In any case, I am concerned about the fact that the assertion is made without substantiating background information, so there is no basis for distinguishing between these items, and further concerned because there is no alternate official source for the underlying data. The CTIA may, in fact, be absolutely accurate in stating that it is aware of no complaints and no problems. But if complaints and problems do indeed exist, what guarantee is there that they will reach the CTIA, or the Commission, for that matter? This point is discussed further in the conclusions.

2. CTIA asserts (their page 3) that cloning and emulation are technologically synonymous, and asserts that they involve precisely the same modifications of the memory in the mobile station, and that attempting to distinguish the two via separate names is merely sophistry. This is technologically incorrect and furthermore this incorrect view leads to attacking the wrong problem in the rule. A legitimate extension emulation requires only a change in the 32 bits at the address of the ESN value in the cellular phone's non-volatile memory, and nothing more. (It may be desirable to also retain a copy of the original ESN value elsewhere as a backup to paper records in case the ESN needs to be changed back for later sale or service of the mobile station, but this is not technologically necessary.) A clone may be modified in this way, and this was a common criminal cloning method in the early 1980s when clones were first uncovered. However, today a clone is very unlikely to be modified in such a simple manner. It is much more likely today that a clone will have extensive changes to the call processing software, and in many cases the original ESN is actually not changed. Of course, the clone will transmit an entirely different number value over the air, often a different ESN value will be transmitted each time the clone phone places a call (so-called "tumbling" clone).

Incidentally, as a result of changing only the ESN, an emulated extension may be converted back to its original ESN by anyone with facilities to change the 32 bits involved, and, of course, the value of the original ESN. In contrast, the only sure way to "clean up" a clone, without knowing the precise type and memory address of all the many changes made, is to replace all of the program memory contents and non-volatile data.

Confusion of Emulated Extension with Cloning Leads to a Rule that Could Allow Clones to Evade Prosecution/Conviction: This continued misunderstanding of the technological distinction between an emulated extension cell phone and a typical "modern" cloned cell phone is reflected in the wording of Rule 22.919, which definitely outlaws legitimate emulated extensions in which only the ESN value is changed, but which gives criminals a significant loophole to evade conviction, since many cloning methods specifically do not change the original factory-set ESN value, but only affect the value transmitted via radio by the cell phone. In many cases, the criminal operator of the clone can cause it to transmit the original valid ESN temporarily (via some special keystroke sequences, for example), so that (assuming the MIN/ESN of the clone is assigned to just that person) the criminal has a technological loophole which could allow the criminal to evade prosecution or conviction. After all, the clone then looks and works just like an unmodified set, and a cursory technological examination of the memory will even disclose the proper ESN in the proper place. Of course, a more thorough examination of the memory will ultimately disclose the other cloning changes, but the rule, as it stands, does not make enforcement easier and more consistent. Just the opposite.

CTIA Should Be Aware of this Distinction: The CTIA should have been fully aware of the technological distinction between the simple change of ESN used for emulated extensions versus the elaborate software modifications designed to produce a well-concealed modification of the transmitted ESN value, or a "tumbling" clone, etc., because the CTIA has funded GTE Laboratories in Waltham, Massachusetts, for several years to study the types of software modifications of cloned cellular sets which have been seized in fraud arrests, and GTE Laboratories have prepared extensive reports on this topic for the CTIA.

I give my own suggestion for the preferred wording for the rule, to avoid giving criminals this particular legal loophole, in the recommendation section.

Analogous Cases of Landline and Cellular Extensions vis-à-vis Fraud: The record in this Docket is replete with arguments about analogies between the ESN as compared to credit card numbers, automobile Vehicle Identification Numbers and license plates, and more. Now we have the issue of whether the cellular extension is analogous to the landline extension. The CTIA asserts that both extensions and clones are technologically identical and that both are, per se, fraudulent use as a result of being technologically identical. I have stated above that they are usually not technologically identical internally, and I assert furthermore that they are not both fraudulent, even in the case where they may use the same technology. Since the confusion in the CTIA's case arises partly from considering incorrect analogies between cellular and landline service, I state a comparison, couched entirely in the terms of landline telephone technology, to illustrate that the

same technology can be used in a manner which is already well recognized, in that context, as being either distinctly permitted or distinctly illegal, depending upon the status of the user, and not depending upon the technology:

Several years ago, I lived in an apartment house and had my telephone plugged in via a plug and jack (the old 4-prong type) in my apartment. A previous tenant in my apartment had also had another jack installed in a public accessible basement storage area, connected to my (originally his) particular telephone line at that location. Once I discovered it, this jack proved to be particularly convenient when I needed to make or receive calls while in the basement storage area.

Now consider the following analogous situations:

2.1 When I take my own telephone extension set to the basement from the bedroom and plug it in, I am enjoying use of my own service, which I pay for. This is true with any telephone set which is technologically indistinguishable from my own set. Use of such a set is analogous to cellular extension emulation.

2.2 If another person, without my knowledge or permission, plugs in a technologically indistinguishable telephone set to this very same basement jack, and makes calls which are billed to me, that is fraud and theft of service. Use of such a set (exactly the same type of set as the previous case) is analogous to cloning.

2.3 To say this again in a slightly different way, cellular radio technology is analogous to the jack on my line which is accessible to the public. If I use it, regardless of which telephone set I use or how many telephone sets I own, this is a legitimate extension use and I pay for any measured call service I use. If an unauthorized person uses a technologically indistinguishable telephone set and makes calls with the intention that they are billed to me without my knowledge and approval, this is fraud and theft of service. The fact that both of us use the same technology to connect to the telephone network is not an invariable indication that I am guilty of fraud (cloning) or that the other person is innocent. In fact, the truth is just the opposite.

Furthermore, if I set this scenario in the 1960s, then I would have to pay the local telephone company a monthly recurring charge for each telephone set extension, regardless of whether I plugged it in at my apartment or in the basement. It was not then permitted to buy and own another telephone set which was technologically indistinguishable from the Western Electric brand telephone set rented to me by the local Bell telephone operating company, and plug it into either jack. This is analogous to the situation desired by the CTIA and by AWS, which would be the result of prohibiting the customer from owning a second set which is technologically indistinguishable from the first. Then the only alternative for a cellular customer who desires multiple sets with the same directory number is Multiple Unit-Same Directory Number (MUSDN) service from the cellular carrier, which despite its deficiencies (e.g. no roaming, no alternate A-B carrier coverage at home, etc.) compared to an emulated extension, has a recurring monthly charge which is typically equal to the recurring charge for the first cellular phone set. The various shortcomings of MUSDN service were discussed in detail in my 1995 report and are summarized in the conclusion section below.

Today, in contrast to the 1960s, I can own and use any telephone set meeting Part 68 specifications, and can plug it in to either jack (if I still lived at that apartment), without paying a monthly recurring charge to the telephone operating company. That appears to me to be absolutely analogous to the situation requested by the former petitioners C2+, and others. In that case I can have additional cellular sets yet pay only one monthly recurring charge, and have full capability from any one of my cellular sets (roaming, alternate A-B carrier service at home, etc.).

Air Interface is the Analogous to the CPE Demarcation: I believe that the most technologically consistent position is to view and treat the air (radio signal) interface between the mobile station (cellular phone) and the base radio as the equivalent, in every regulatory way, of the demarcation point in landline service between the customer provided equipment (CPE) and the network provider's equipment, due to the almost identical technological properties of these two interfaces. All other approaches (including the false distinction by the CTIA regarding simultaneous use of extensions on the same channel, discussed below) are technologically inconsistent and appear to me to be a weak attempt to fit the contrary facts into a bad theory.

Further Distinguishing Identification is Desirable and Practical: Although I have referred above to "technologically indistinguishable" cellular phones, I believe that it is advantageous for several reasons (repair and replacement, upgrading, etc.) to have a separate distinguishing identifier from the MIN and ESN for cellular phones with the same MIN, ESN and Authentication A-key, etc. This is described in my 1995 report as well. This is done in the European and related PCS systems by means of a physical equipment serial number (different from the ESN) which can be remotely interrogated under special circumstances. That is one of several methods which are readily adaptable to the US 800 MHz cellular band. Other methods include the use of some of the existing reserved bits in existing call processing messages, or defining certain previously unassigned call processing function codes to identify alternate 800 MHz extension sets, etc. The optimum choice should be set by an appropriate standards committee, where all the parties are represented, although I suggest the first method in my recommendations below merely to give a definite example already proven by European systems.

3. The CTIA asserts (their pages 3-4) that the analogy between landline extension phones and cellular emulated extension phones is technologically invalid because they assert that true extensions share one and only one transmission path linking the various extensions to the telephone company's end office or network. The distinction which the CTIA attempts to draw is technologically incorrect in several ways, or at best a half-truth. Furthermore, the point is not technologically relevant because the opposite case of landline station sets exist which also have identical technological limitations (as claimed by the CTIA) requiring only one set to be used at a time on a transmission channel, yet no suggestion has been made (at least, since the 1960s) that the consumer pay an extra monthly recurring fee to the landline carrier for such equipment.

3a. Two or more portable analog handset type cellular phones (all of which have a pre-existing standard feature called discontinuous transmit - DTx - a form of voice controlled transmitter switch on or off, which is designed to conserve battery power) can indeed be caused technologically to share the precise same cellular radio channel in the same cell. Sets equipped with DTx capability are the most popular in sales and they now constitute the majority of sets in field use. In a two-set one-channel DTx situation, only one mobile customer can speak at a time, since simultaneous speech will cause garbling. However, this is precisely like two landline extension users coordinating their speaking so that they do not speak simultaneously, which also causes garbling. This technological point of simultaneous channel use by DTx mobiles was extensively investigated in the TIA standards committee at the request of the CTIA, among many other proposals to increase the system capacity of cellular systems in the late 1980s. It was not technologically developed because, while technologically feasible, it makes the cellular system operate as a radio dispatch system (one base station in simultaneous contact with multiple mobile radios on the same cell RF channel), which is legally prohibited for Part 22 cellular service. Therefore, its absence in normal cellular operation is a legal, not a technical, restriction, which is begging the question by asking for a legal restriction based on the existence of a legal restriction, rather than pointing out a true technological distinction.

To give a complete and fair answer, we must say also that, in two particular cases, DTx operation does not occur. Some older higher powered vehicle mounted cellular mobile phone sets do not have DTx capability and always transmit continuously. Therefore, if two of these were set to operate on the same radio channel in the same cell, the stronger transmitter signal (as measured at the base receiver) would dominate the transmission path and the weaker one would not be heard (due to the well-known "capture effect" of FM radio). In addition, some very few base stations do not have the proper up-to-date call processing software to handle DTx operation, and they can send a signal to force all mobile units to transmit continuously (of course, while running down their batteries more rapidly as well). Both mobile receivers on the same channel could, of course, simultaneously receive the conversation in non-DTx mode under any circumstances. Therefore, in all fairness to the assertion of the CTIA, there are some cellular mobile sets which cannot share the same transmission channel in the same cell simultaneously, so perhaps we could describe their assertion as a half truth.

3b. The new CDMA cellular mobile sets (TIA Standard IS-95), which are now undergoing field trials in several cities and are poised for commercial introduction, share the same unique single transmission channel between all the CDMA mobile units in each cell (as many as 64 simultaneously). The digitally coded speech signals from all these different CDMA cellular mobile sets are separated by means of their "tagging" with separate CDMA identification codes, only after they have been received by one single common shared base receiver. All the transmit signals are likewise combined and share one single common base transmitter. In addition, there are some authorities who would argue that the IS-54 TDMA mobile sets share the same transmission channel in the same cell, although not instantaneously shared.

3c. In contrast to the assertion by CTIA that landline extensions are technologically distinct from cellular extensions because the landline extensions all access the same transmission path simultaneously while cellular extensions cannot, consider the following widely used landline telephone services which cannot operate with multiple devices accessing the same transmission path simultaneously:

3c.1. Facsimile machines (FAX)

3c.2. Data Modems

3c.3. Integrated Services Digital Network (ISDN) for voice or data

In addition, each of these devices cannot work properly when there is also a voice telephone off-hook (in use) on the same line, even if there is no conversation on that telephone. Many of us have had the unpleasant experience of a data or fax call being interrupted due to another voice telephone on the same line being taken off-hook.

Each one of these three example landline devices has precisely the same restriction as cellular emulated extension services and MUSDN on a single radio channel, namely: The user may own and use multiple instances of each type of device, so long as only one is connected and powered up on the transmission path (in this case the telephone wires) at one time. Attempting to use more than one on the same transmission path simultaneously will

produce either mutual interference or a signal from only one will get through, precisely like the case of non-DTx cellular phones.

4. Finally, the CTIA again asserts (their page 4) the claim in connection with the above assertions, that use of emulated extensions must, perforce, be uncontrollable (while, by implication, but never stated by them, the similar MUSDN services offered by cellular carriers are somehow not) and that the use of extension phones will interfere with detection of an actual clone. All of these matters were rebutted in detail in my 1995 report, with which the CTIA agreed without reservation in the July 1995 meeting. I refer the reader to that report for a more complete rebuttal of this claim with regard to both the technological and operational aspects of the alleged interference with fraud detection and enforcement. More discussion of MUSDN is given below in several sections, particularly section 12.

5. AT&T Wireless Services (AWS) first makes a number of legal assertions which I will not comment on, limiting my comments in this filing to only technological issues. In addition, AWS asserts a number of technological problems with improper simultaneous use of multiple extensions (their pages 7-9 and 10-12), but, like CTIA, do not also point out that each and every one of these restrictions on simultaneous use must also be applied to a MUSDN sets as well. AWS complains that the lack of a limit on the number of emulated extensions which a single customer may possess will invariably lead to a high level of false network signals of various types, but Tim Fitzgibbon, attorney for C2+, in a previous letter (Aug. 10, 1995) to Regina M. Keeney, of the Wireless Telecommunications Bureau of the Commission, has suggested rules and procedures to establish a reasonable limit on the number of extensions for each MIN/ESN, which offer I understand is backed by all the emulated extension providers who have appeared before the Commission on this matter. I agree that the Commission should set a limiting number and I give further suggestions in my recommendations section.

"One Free Cloner" Call Argument is Technologically False: In regard to the assertion by AWS (their pages 9 and 10-12) that possible simultaneous emulated extension phone use is uncontrollable, AWS asserts (page 9 and 10-12) that "...there will always be one free cloner call available on the network because carriers will never have the capability of determining whether the second call is a clone or an extension, absent extraordinarily costly procedures to verify usage with the customer ...". This point was fully addressed and rebutted in my 1995 report, which AWS also agreed to in the July 1995 meeting. Without repeating all the rebuttal material on that point, let me indicate that use of a PIN and/or authentication, to give only two examples, are two preferable methods which are both eminently suitable for this particular purpose, and are already extensively available, and which are not -- according to the overwhelming majority view in the industry -- "extraordinarily costly." None of these anti-fraud procedures and technologies were put in place to address the use of emulated extensions, so their cost, such as it is, cannot be blamed on the presence of emulated extensions. I find absolutely no technological or operational justification for AWS to claim that they must give away "one free cloner call."

Misapplication of Quotation from Levine 1995 Report: In this same section (footnote 21 on page 11) AWS also misquotes and misapplies my 1995 report by applying my statement showing the limitation of using only "velocity" or "time-place" tests in such a case, where the preferred method is clearly use of a PIN or authentication. This misquotation is apparently directed towards making it appear that I agree that there is a higher level of fraud susceptibility for emulated extensions in general. That is untrue, and I did not say that. Rather, I would say that there is a higher level of fraud susceptibility in this case, but only when a carrier chooses to use an inappropriate method of fraud prevention.

6. AWS asserts (pages 9 and 12-13) that "...techniques such as RF 'fingerprinting' which creates a distinct RF profile to validate calls for each phone, will not work with extension phones without significant alterations in the current cellular system -- changes again apparently C2+ would have the carrier bear."

Modifications to RF Fingerprint/Signature Systems to Accommodate Extensions are both Simple and Straightforward and Affect Only the RF Fingerprint/Signature Equipment, Not the Cellular Network: The assertion by AWS is technologically incorrect. Furthermore, almost every aspect of the operation of an RF fingerprint or RF signature system which is a part of normal operations and which already exists, is described by AWS as if it were a complex and particularly vexing problem situation caused by emulated extensions and requiring major costly development. For example, all RF signature systems automatically "enroll" new mobile station "fingerprints" the first time setup channel radio signals are received from each particular mobile set in that cell by the RF signature equipment. This is an automatic feature of these systems, and the modification required for emulated extensions is that the RF signature system would require human input in advance to identify the existence of multiple extensions with some particular MIN/ESN values.

Human Input for RF Signature/Fingerprint Activation of Multiple Extension Sets is Actually Less than for MUSDN Sets: In a properly designed RF Signature/Fingerprint system, the relevant part of the human input for enrolling a customer with one cellular phone consists of typing in the MIN, the ESN, and the digit "1" (or perhaps no digit entry) into a data base. In contrast, for a customer with three (for example) emulated extensions, the human input for this case requires typing the MIN, the ESN and the digit "3." For further contrast, the input for enrolling a customer with two MUSDN sets consists of the MIN, ESN and digit "1" for the first set, and then the MIN (same value), the ESN (different from the first)

and the digit "1" for the second MUSDN set. All other human input regarding the RF Signature/Fingerprint aspect is the same regardless of the single phone vs. emulated extension vs. MUSDN issue. This is stated in detail to rebut the later claim by AWS that a greater labor force would be required because of alleged vastly greater data entry for emulated extensions. In addition, there is additional input "paperwork" on the part of the carrier for activating a second MUSDN set which is more than the corresponding paperwork for an extension set because the switch produces two billing data record streams for MUSDN sets which must be merged before the final customer bill is printed, never mentioned by AWS.

Handling of Suspected Cloning is Identical for Single Phone and for Emulated Extensions: Today, RF signature equipment indicates a second distinguishable RF "fingerprint" as something special, when it was programmed to anticipate only 1 cellular telephone set with a particular MIN/ESN. In the case of programming for two (for example) extension sets with the same MIN/ESN, the RF signature equipment will indicate a third distinguishable RF "fingerprint" as something special. In both special cases, the RF signature equipment then finds that there is one more cellular mobile set present than it was programmed to find. At this point, other external actions must be taken to determine which sets belong to the legitimate subscriber and which to an illegal clone. Although I will not describe these steps here for reasons described below, further examination of the process will disclose that the rest of the process is identical in both cases. This is not a complex problem.

Modifications to RF Signature/Fingerprint Equipment to Accommodate Emulated Extensions is Neither Complex Nor Disruptive: The cross reference of multiple extension phones in the data base is not a new development, and is not complex. It is of the same level of alleged "complexity" as, and must be done in any case, for the support of MUSDN phones. Maintenance and backward compatibility of such a system for existing RF fingerprints already in the system is not complex. Absolutely nothing fundamental about the RF signature systems, nor their existing data storage or methodology, will be rendered obsolete. The only actual significant impact of multiple extensions on an RF signature system will be the storage of the individual "fingerprint" data for multiple phones for an extension customer; one phone for an "ordinary" customer versus two phones for a MUSDN customer. I purposely do not describe here the supporting information to explain in detail why these modifications are not complex and costly for two reasons. First, for reasons of length. Second, to avoid placing in a public document information about the detailed internal operations of anti-fraud systems which could be of value to persons who would abuse this information. This latter point is also addressed in my conclusion section. I will, however, give a minimal amount of background to explain why some of the more egregious statements are incorrect.

More information regarding how an RF fingerprint or RF signature system would handle multiple extension phones (and MUSDN phones for that matter) is given in my 1995 report. It is neither complex nor would significant alterations in the RF signature equipment software be required. The assertions by AWS that the cellular network or system would require significant and complex alterations is technologically incorrect for the following reasons:

6.1 The interface between the RF signature equipment is generally (depending upon the design of the RF signature equipment vendor) one of two types. The simplicity of this interface to the cellular network and the fact that no significant modifications of the cellular network are needed in order to implement RF signature equipment installation is one of the major advantages claimed repeatedly by all of the vendors of such equipment. Surely any person involved with fraud control has heard these claims by the vendors. The interfaces are:

6.1.1 A simple "go/no-go" electrical signal to the cellular base station or Mobile-service Switching Center (MSC) to either continue or abort the call setup for the cellular phone being examined by the RF signature equipment, or

6.1.2 A "radio" interface which has no actual wire or data link connection between the RF signature equipment and the cellular network. The RF signature equipment prevents a cellular phone, which it identifies as invalid, from proceeding to set up a call by producing selective radio interference which causes the MSC to abandon the call.

Networking Development Problems Related to RF Signature/Fingerprint Technology is Pre-existing and Not Related to Extensions: In this connection, it is well known in the industry that there are significant technological development problems involved in networking together RF signature equipment at different cells. The problem is even greater when equipment from different vendors is considered. However, one should not confuse this well-known problem between RF signature equipment at different cell sites (which is a basic problem related to the technology of RF signature methodology, complicated by different vendors with distinct proprietary analysis methods requiring different detection parameters) with the problem alleged by AWS of significant alterations in the current cellular system. These problems have nothing whatsoever to do with the presence of cellular extension sets. All new systems go through a development shakedown phase, and these systems are no exception. Furthermore, regardless of the complexity of the eventual development of the networking between the RF Signature/Fingerprint equipment, this has no impact on the cellular network. The interface between these two networks remains as simple as described above.

7. AWS alleges (page 9-10) that authentication technology renders authentication phones unusable in the home area [of AWS's network, emphasis added]. Further, AWS claims that to accommodate emulated extensions carriers would "...either have to re-engineer the authentication industry standard or perform services for C2+ customers to ensure that their 'cloned' authenticated phones work on the network. Once again, C2+'s proposal is all risk and liability for the carrier and all reward for itself." **Each and every one of these technological assertions by AWS is false.**

7.1 The allusion by AWS to a distinction between authentication in the home area versus roaming is the key to several important technological considerations. It is necessary to give some history here to explain who, what and why. When the authentication algorithm was developed in the standards committee in 1989-91, the question arose regarding whether the standard should require all implementors to place all the secret authentication data on a separate silicon chip with a separate microprocessor, as opposed to implementing it in the same processor and memory as other call processing software (so-called "one-piece"). A separable chip would have been slightly more costly to manufacture (perhaps a difference of one dollar or more), but would have effectively unbreachable security against physical attack (disassembly and electrical probing) on the cellular phone, since the secret information needed for authentication (A-key, etc.) could go in, but will never come out, and cannot be extracted by means of test or measuring equipment! Only identification numbers derived from the internal secret information, and which are furthermore different on each occasion of use and which cannot be used to determine the underlying secret numbers, do come out. Furthermore, optimum security, speed and accuracy in a separable chip implementation would require putting all the identification numbers for the mobile telephone (such as the MIN and ESN) in the separable chip, rather than in the main memory of the cell phone. This is all well proven in the European systems and the US PCS systems derived from them.

7.2 Manufacturers were unanimous in the position that they would not individually increase the cost of their cellular mobile sets compared to others, unless all the manufacturers were mandated to offer the same level of high security afforded by a separable chip, as was already underway in the European GSM cellular standards. The cellular carriers were all represented at these meetings, including in particular the present two petitioners CTIA (with its own appointed representatives, separate from any individual carrier) and AWS (then called McCaw Cellular). The carriers wanted the lower cost of a "one-piece" implementation, and were willing to sacrifice the unbreachable security of the separable chip. Because various scenarios of increased susceptibility to physical attack on the authentication data for a "one-piece" implementation are possible, although difficult to carry out, a call counter was suggested as a remedy by several of the technologists at these meetings. The carrier representatives initially objected to the call counter, or at least wanted it to be totally separate and optional, because they were not sure that the cellular data communications network between the MSCs could update the needed call counter data rapidly enough for the case of roaming cellular mobile sets. The technologists who proposed the call counter pointed out to the carriers that experience indicated that a very large part of their fraud losses occurred with roaming situations, and an optional feature might be too tempting to omit, thus very slightly increasing the susceptibility to roamer fraud. The matter was only settled when the technology experts on the committee agreed to write the industry authentication standard so that the use of the call counter is optional, so any operators who were not confident of the data transmission speed of their inter-MSC cellular data communication links could opt to omit the additional variable identifier.

I repeat this history to point out several important aspects of the industry standard authentication algorithm:

a. The industry standard authentication algorithm, if implemented in a separable chip, has no security need for the call counter. The call counter is included in the authentication standard, as an option only, to improve the security of a "one-piece" implementation against a possible but improbable physical attack on the cellular phone, followed by returning that same phone to normal service in the hands of its legitimate owner without the owner being aware of the success of the attack. Whether optionally used or optionally omitted by the carrier, no change whatsoever in the industry standard algorithm is required to support emulated extensions. No re-engineering (of the network, the air interface, the data bases, etc. etc.) is required. There is no particular reward for C2+ or any other emulator for the network supporting the industry standard authentication algorithm, and no added risk for the operators like AWS beyond what exists at their own explicit request and choice in the existing standard and their own network.

b. The call counter is apparently already omitted by AWS, in particular, for roaming service, where historically fraud losses have been more severe, and is used by them only in the home area, (as accented by my underlining of their quoted text). Given this position of AWS, it is completely inconsistent for them to argue that there is an unacceptable increase in risk for them to support extensions by this industry standard method. Furthermore, even in the home area, AWS has the option of using the call counter for all home customers except extension users, if they so desire. In that way, any alleged

greater risk falls only on emulated extension customers, contrary to AWS assertion on their pages 10 and 14. Furthermore, if the wording of Rule 22.919 were altered to permit transfer of the ESN, an emulated extension customer would possibly have available in the near future a separable chip implementation of authentication in his/her cellular phone, thus removing completely the alleged slight extra risk (for both the customer and AWS) arising from the improbable physical attack on the cellular phone.

7.3 AWS asserts (their page 13-14) a chain of technologically incorrect statements regarding the industry standard authentication algorithm and their interpretation of the position of C2+ regarding these points. In the following paragraphs I will attempt to set straight the technological facts and state the correct consequences. These succeeding factual paragraphs contradict, almost sentence by sentence, the technologically false statements in the last two paragraphs from AWS on their page 13 and the first paragraph on page 14, with some exceptions as noted.

- a. Contrary to the dates given by AWS, the industry authentication standard was completed in 1991. It was available in IS-54 compatible mobile stations within 10 months thereafter. There was indeed a 4 year (or longer) delay before software became generally available for cellular switches, but this was not due to the complexity of the development. In fact, some vendors of network components involved in authentication have not even cross-verified interworking with other vendors to date. The delay in implementation for switches was due primarily to a longstanding state of confusion and indecision on the part of major carriers regarding the relative priority of authentication vis-à-vis other network software developments, combined with a limit on the resources of software development and testing which was available from the MSC switch manufacturers. The carriers did not ask the manufacturers to elevate the priority of authentication software, but did demand other features. There is much more to this story which would be out of place in this context.
- b. The industry standard indeed integrates the ESN as part of the algorithm, as AWS states. However, nothing in the industry standard prohibits moving or copying/duplicating the authentication process and related data (MIN, ESN, A-key, etc.) from one cellular set to another. That is perfectly feasible technologically, with no change whatsoever in the algorithm nor in the cellular network. The only prohibition is a legal one, namely Rule 22.919 in its present form. Again, bear in mind that by prohibiting such a transfer, there is a sacrifice of the unbreachable security level afforded by a separable chip implementation. Although this is standard in European GSM cellular technology and derived systems (e.g. PCS-1900), manufacturers are understandably unwilling to put the more costly separable chip implementation into their US cellular set in a competitive market when other manufacturers are not compelled to offer an equally high level of security, and there is no other corresponding benefit such as portability of the authentication to another extension of the same customer.
- c. Transferring the entire authentication algorithm in the form of a separable chip (which would include the MIN, ESN, A-key, call counter described above, etc etc) would (contrary to AWS's assertion) cause the destination cellular phone with this transferred information to operate perfectly in AWS's network, local area or roaming or both. Of course, such a transfer is prohibited by the present Rule 22.919.
- d. In addition, if we consider a "one-piece" implementation of the authentication algorithm (feasible in most existing cellular sets by modification of the software/firmware) in which there is no attempt to retain the additional variable identifier, two cellular phones having the same other data values such as MIN, ESN, A-key, etc., would indeed operate perfectly on the AWS network out of the home area (that is, while roaming) with no changes in the AWS network. If the option of omitting the call counter was set selectively for emulated extension users only, as previously indicated, there would be complete service for both sets in the home area as well, with no reduction or change in service for non-extension sets compared to the present AWS practices. Although this implementation also is prohibited by the present Rule 22.919, such sets would be highly immune to cellular fraud (to the extent explained before) and would achieve the industry's stated objective of elimination of fraud.
- e. AWS asserts that C2+ and my 1995 report argue that the Commission should reject the current industry authentication standard and introduce a different standard, consequently requiring a complete re-engineering of the cellular network to benefit C2+ and penalize the carriers with a large cost. This assertion by AWS is totally incorrect, both on the factual basis, and it is also a misquote. I am absolutely at a total loss to comprehend how anyone can read these implication into the previous documents by myself or by C2+. Although I will state my suggestions again in the